

1 CLAIM AMENDMENTS

2 What is claimed is:

3 1. (Original) A method for generating a key pair, the method
4 comprising:

- 5 - forming a private key which includes at least one
6 enhancing key; and
7 - forming a public key which includes a commitment to said
8 at least one enhancing key, wherein the public key and the
9 private key form the key pair.

10 Claim 2. (Original) The method as recited in Claim 1, wherein the
11 step of forming a public key comprises computing a function on a
12 commitment to an enhancing key and a 1-time public key.

a1 13 Claim 3. (Original) The method as recited in Claim 1, wherein the
14 enhancing key is randomly chosen.

15 Claim 4. (Original) The method as recited in Claim 1, further
16 comprising employing the enhancing key in a process.

17 Claim 5. (Original) A method as recited as in Claim 4, wherein
18 the process performs a hash calculation.

19 Claim 6. (Original) A method as recited in Claim 1, further
20 comprising computing a certificate for the public key.

21 Claim 7. (Original) A method as recited as in Claim 1, wherein
22 the commitment is a TCR commitment.

1 Claim 8. (Original) The method as recited in Claim 7, further
2 comprising employing the enhancing key in a process.

3 Claim 9. (Original) A computer program product comprising a
4 computer usable medium having computer readable program code
5 means embodied therein for generating a key pair, the computer
6 readable program code means in said computer program product
7 comprising computer readable program code means for causing a
8 computer to effect the steps of claim 1.

9 Claim 10. (Original) A method of forming a TCR commitment
10 comprising:

11 - providing a commitment for a first string, and
12 - applying a TCR function to a second string that includes the
13 commitment.

14 Claim 11. (Original) A method as recited in Claim 10, wherein the
15 step of applying includes:

16 - choosing a random key for the TCR function.
17 - evaluating the TCR function on the random key and the second
18 string.

19 Claim 12. (Original) A method as recited in Claim 11, wherein the
20 TCR function is a basic cryptographic primitive.

21 Claim 13. (Original) A method as recited in Claim 12, wherein the
22 cryptographic primitive is the SHA-1 compress function.

23 Claim 14. (Original) A method as recited in Claim 10, wherein the
24 step of applying forms a TCR function output which is 80 bits
25 long.

1 Claim 15. (Original) An article of manufacture comprising a
2 computer usable medium having computer readable program code
3 means embodied therein for generating a key pair, the computer
4 readable program code means in said article of manufacture
5 comprising computer readable program code means for causing a
6 computer to effect the steps of claim 1.

7 Claim 16. (Original) A method as recited in Claim 10, further
8 comprising employing the TCR commitment in an enhanced commitment
9 based signature scheme.

10 Claim 17. (Original) A method as recited in Claim 1, wherein the
11 public-private key pair is used a bounded number of times.

12 Claim 18. (Original) A method as recited in Claim 17, where the
13 bounded number is 36.

a' 14 Claim 19. (Original) A method as recited in Claim 12, wherein the
15 TCR function is a TCR hash tree based on a basic cryptographic
16 primitive.

17 Claim 20. (Original) A method as recited in Claim 1, further
18 comprising employing the key pair in a commitment based signature
19 scheme.

20 Claim 21. (Original) The method as recited in Claim 4, wherein
21 the process is a 36-time signature scheme.

22 Claim 22. (Original) A method as recited in Claim 10, further
23 comprising employing the TCR commitment in an E-commerce
24 protocol.

25 23. (currently amended) A method comprising:

1 generating a TCR commitment opening function for extracting a
2 data string committed to by at least one TCR commitment message,
3 utilizing a corresponding TCR opening string for each said at
4 least one TCR commitment message, and

5 wherein the step of generating the TCR commitment opening
6 function includes:

7 receiving a TCR commitment message and the corresponding TCR
8 opening string;

a' 9 extracting a hash value and a key from said TCR commitment
10 message; and

11 extracting a regular opening string and a regular commitment
12 message from said corresponding TCR opening string,

13 computing the TCR hash function with said key and said
14 regular commitment message forming a result value, and

15 comparing said result value with said hash value;

16 if the step of comparing results in a compare, applying said
17 regular opening commitment function on said regular opening
18 string and said regular commitment message to produce said data
19 string.

20 Claim 24. (Original) An article of manufacture comprising a
21 computer usable medium having computer readable program code
22 means embodied therein for generating a TCR commitment opening
23 function for extracting a data string committed to by at least

DOCKET NUMBER: YOR919990229US2

-5/17-

1 one TCR commitment message, the computer readable program code
2 means in said article of manufacture comprising computer readable
3 program code means for causing a computer to effect the steps of
4 claim 23.

5 Claim 25. (Original) A computer program product comprising a
6 computer usable medium having computer readable program code
7 means embodied therein for causing generation of a TCR commitment
8 opening function, the computer readable program code means in
9 said computer program product comprising computer readable
10 program code means for causing a computer to effect the steps of
11 claim 23.

ai 12 Claim 26. (Currently amended) A method as recited in Claim 10,
13 wherein the step of generating the TCR commitment function
14 includes:

15 receiving a data string to be committed and receiving secret
16 information, if any, in a regular commitment scheme;

17 computing a regular commitment message using said regular
18 commitment scheme upon both said data string and said secret
19 information;

20 randomly selecting a key for said TCR function;

21 computing said TCR function on said key and said regular
22 commitment message and obtaining a resulting hash value;

23 forming a TCR commitment message including said resulting
24 hash value and said key, said TCR commitment message being an
25 output of said TCR commitment function.

1 Claim 27. (Original) A method as recited in Claim 26, further
2 comprising saving said regular commitment message.

3 Claim 28. (Original) A method as recited in Claim 27, wherein the
4 step of saving is performed for a commiter.

5 Claim 29. (Original) A method comprising:

6 generating a TCR de-commitment function for de-committing at
7 least one TCR commitment message employing a TCR function and a
8 regular commitment scheme used in generating said at least one
9 TCR commitment message.

a 10 Claim 30. (Original) A method as recited in Claim 29, wherein the
11 step of generating the TCR de-commitment function includes:

12 receiving a data string committed and receiving secret
13 information used in generating said at least one TCR commitment
14 message if any;

15 receiving a regular commitment message computed as part of
16 generation of said at least one TCR commitment message;

17 computing the regular de-commitment function on using said
18 regular commitment message, said data string and said secret
19 information and generating a regular opening string;

20 forming a TCR opening string including said regular opening
21 string and said regular commitment message, said TCR opening
22 string being an output of said TCR de-commitment function.

23 Claim 31. (currently amended) A method comprising:

1 generating a TCR commitment function by employing a TCR function
2 and utilizing a regular commitment scheme; wherein the step of
3 generating the TCR commitment function includes:

4 receiving a data string to be committed and receiving secret
5 information, if any, in said regular commitment scheme;

6 computing a regular commitment message using said regular
7 commitment scheme upon both said data string and said secret
8 information;

9 randomly selecting a key for said TCR function;

10 computing said TCR function on said key and said regular
11 commitment message and obtaining a resulting hash value;

a 12 forming a TCR commitment message including said resulting
13 hash value and said key, said TCR commitment message being an
14 output of said TCR commitment function.

15 Claim 32. (Canceled)

16 33. ((currently amended) The method as recited claim 23 wherein
17 reporting an error if the step of comparing results in a
18 non-compare, and reporting a non-error if the step of comparing
19 results in a compare.

20 Claim 34. (Canceled)

21 Claim 35. (currently amended) A method comprising:

22 constructing a TCR commitment scheme comprising:

1 a TCR commitment function;
2 a TCR de-commitment function; and
3 a TCR commitment opening function,

4 by employing a TCR function and a regular commitment scheme,
5 wherein the step of constructing the TCR commitment function
6 includes:

7 receiving a data string to be committed and receiving secret
8 information if any in said regular commitment scheme;

9 computing a regular commitment message using said regular
10 commitment scheme upon both said data string and said secret
11 information;

a 12 randomly selecting a key for said TCR function;

13 computing said TCR function on said key and said regular
14 commitment message and obtaining a resulting hash value; and

15 forming a TCR commitment message including said resulting
16 hash value and said key, said TCR commitment message being an
17 output of said TCR commitment function.

18 Claim 36. (Original) An article of manufacture comprising a
19 computer usable medium having computer readable program code
20 means embodied therein for generating a TCR commitment function,
21 the computer readable program code means in said article of
22 manufacture comprising computer readable program code means for
23 causing a computer to effect the step of claim 25.

24 Claim 37. (Original) A method as recited in Claim 25, wherein the
25 TCR function is a basic cryptographic primitive.

DOCKET NUMBER: YOR919990229US2

-9/17-

1 Claim 38. (Original) A method as recited in Claim 37, wherein the
2 cryptographic primitive is the SHA-1 compress function.

3 Claim 39. (Original) A method as recited in Claim 26, wherein
4 said resulting hash value is 80 bits long.

5 Claim 40. (Original) A method as recited in Claim 25, wherein the
6 TCR function is a TCR hash tree based on a basic cryptographic
7 primitive.

8 Claim 41. (Original) A method as recited in Claim 35, further
9 comprising employing the TCR commitment scheme in an enhanced
10 commitment based signature scheme.

a 11 Claim 42. (Original) A method as recited in Claim 35, further
12 comprising employing the TCR commitment scheme in an E-commerce
13 protocol.

14 Claim 43. (Currently amended) An article of manufacture
15 comprising a computer usable medium having computer readable
16 program code means embodied therein for causing formation of a
17 TCR commitment message, the computer readable program code means
18 in said article of manufacture comprising computer readable
19 program code means for causing a computer to effect the steps of
20 claim 31.

21 Claim 44. (Original) An article of manufacture comprising a
22 computer usable medium having computer readable program code
23 means embodied therein for generating a TCR de-commitment
24 function, the computer readable program code means in said
25 article of manufacture comprising computer readable program code
26 means for causing a computer to effect the steps of claim 29.